

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A proactive operating environment that includes a group of proactive servers communicating over a network; each proactive server (PS_I) comprising:

a storage that includes a non erasable part that stores at least a public, non proactive related, key V_{start}^I ; said storage further includes an erasable part for storing private and public data; said proactive server is further associated with a discardable one-time private key S_{start}^I that corresponds to said public key V_{start}^I ; said proactive server is further associated with configuration data C ;

a processor for providing at least proactive services to applications;

the proactive server is associated with a group public proactive key V_{CERT} common to said group of proactive servers and a share S_{CERT}^I of a corresponding private proactive key S_{CERT} ;

the processor is operative to invoke initialization procedure for generating restore related information;

the processor is further operative to invoke a restore procedure for utilizing at least said public, non

proactive related, key V_{start}^I and said restore related information for restoring at least said public proactive key V_{CERT} .

2. (Original) The system according to Claim 1, wherein said restore procedure is invoked by refresh procedure.

3. (Original) The system according to Claim 1, wherein said non erasable part of the storage being a ROM memory module.

4. (previously presented) The system according to Claim 1, wherein said applications are at least one of the following:

Secure logging, Secure end-to-end communication, Timestamping, Certificate authority, Key recovery, Voting, Trading, Database, Operating system, Access control mechanisms, Secure Commerce.

5. (Original) The system according to Claim 1, wherein said restore related information includes restore related self information.

6. (Original) The system according to Claim 1, wherein said restore related information includes restore related others' information.

7. (previously presented) The system according to Claim 5, wherein said restore related self information includes $M_I = S^I_{start} (V_{Cert}, C)$.

8. (previously presented) The system according to Claim 6, wherein said restore related others' information includes $(S_{Cert}(M), M)$.

9. (previously presented) The system according to Claim 1, wherein said initialization procedure includes:

- (i) input for receiving at least configuration data C , public non-proactive related key V^I_{start} and discardable one time private key S^I_{start} ;
- (ii) the processor generating a set of keys $S_I(0)$, $V_I(0)$, $E_I(0)$, $D_I(0)$;
- (iii) broadcasting said set of keys except $D_I(0)$ over the network to the rest of the servers ($1..i-1, i+1..n$) in the group, so as to authenticate and encrypt the network channel;
- (iv) the processor generating the group public proactive key V_{Cert} and a share (S^I_{CERT}) of corresponding private proactive key S_{CERT} ;
- (v) the processor generating restore related self information that includes $M_I = S^I_{start} (V_{Cert}, C)$;
- (vi) discarding the one-time private key S^I_{start} ;

- (vii) broadcasting M_I to all servers in the group, and receiving M_J from all respective SP_J servers in the group; the processor concatenating said $M_1..M_N$ so as to construct M ;
- (viii) the processor generating a joint signature $(S_{Cert}(M), M)$ that forms part of said restore related others' information; and
- (ix) broadcasting the joint signature $(S_{Cert}(M), M)$.

10. (previously presented) The system according to Claim 1, wherein said recover procedure includes:

- (i) the processor extracting V_{start}^I ;
- (ii) the processor extracting M_I from M ;
- (iii) the processor constructing V_{Cert} by applying V_{start}^I to M_I ;
- (iv) the processor validating M by applying V_{CERT} to the joint signature part $(S_{Cert}(M))$; if the result matches M then the server becomes operational; sending M and $S_{Cert}(M)$ to all the group servers;
- (v) if, on the other hand, M is invalid, then waiting the receipt of another joint signature and in response repeating said (ii) to (iv).

11. (previously presented) The system of Claim 1, wherein an initialize procedure is configured to generate restore related information.

12. (previously presented) The system of Claim 1, wherein a restore procedure is configured to utilize at least said public, non proactive related, key V_{start}^I and said restore related information for restoring at least said public proactive key V_{CERT} .

13. (Currently Amended) A method for providing a proactive security in proactive operating environment; wherein the proactive operating environment includes a group of proactive servers communicating over a network; the method comprising performing the following in respect of each proactive server (PS_I) comprising:

~~a storage that includes storing in a non erasable part that stores at least a public, non proactive related, key V_{start}^I ; said storage further includes an erasable part for storing, in an erasable part private and public data; said proactive server is further associated with providing~~ a discardable one-time private key S_{start}^I that corresponds to said public key V_{start}^I ; ~~said proactive server is further associated with providing~~ configuration data C ;

a processor for providing at least proactive services to applications;

~~the proactive server is associated with providing a group public proactive key V_{CERT} common to said group of proactive servers and a share S^I_{CERT} of a corresponding private proactive key S_{CERT} ; the method further including:~~

invoking an initialization procedure for generating restore related information; and

invoking a restore procedure for utilizing at least said public, non proactive related, key V^I_{start} and said restore related information for restoring at least said public proactive key V_{CERT} .

14. (Original) The method according to Claim 13, wherein said restore procedure is invoked by refresh procedure.

15. (previously presented) The method according to Claim 13, wherein said non erasable part of the storage is a ROM memory module.

16. (previously presented) The method according to Claim 13, wherein said applications are at least one of the following:

Secure logging, Secure end-to-end communication, Timestamping, Certificate authority, Key recovery, Voting,

Trading, Database, Operating system, Access control mechanisms,
Secure Commerce.

17. (Original) The method according to Claim 13, wherein said restore related information includes restore related self information.

18. (Original) The method according to Claim 13, wherein said restore related information includes restore related others' information.

19. (previously presented) The method according to Claim 17, wherein said restore related self information includes $M_I = S_{start}^I (V_{Cert}, C)$.

20. (previously presented) The method according to Claim 18, wherein said restore related others' information includes $(S_{Cert}(M), M)$.

21. (previously presented) The method according to Claim 13, wherein said initialization procedure includes:

- (i) receiving at least configuration data C , public non-proactive related key V_{start}^I and discardable one time private key S_{start}^I ;
- (ii) generating a set of keys $S_I(0)$, $V_I(0)$, $E_I(0)$, $D_I(0)$;
- (iii) broadcasting said set of keys except $D_I(0)$ over the network to the rest of the servers ($1..i-1, i+1..n$) in

- the group, so as to authenticate and encrypt the network channel;
- (iv) generating the group public proactive key V_{Cert} and a share (S^I_{CERT}) of corresponding private proactive key S_{CERT} ;
 - (v) generating restore related self information that includes $M_I = S^I_{Start} (V_{Cert}, C)$.
 - (vi) discarding the one-time private key S^I_{Start} ;
 - (vii) broadcasting M_I to all servers in the group, and receiving M_J from all respective SP_J servers in the group; the processor concatenating said $M_1..M_N$ so as to construct M ;
 - (viii) generating a joint signature ($S_{Cert} (M), M$) that forms part of said restore related others' information; and
 - (ix) broadcasting the joint signature ($S_{Cert} (M), M$).

22. (currently amended) The method according to Claim 13, wherein said ~~recover~~ restore procedure includes:

- (i) extracting V^I_{Start} ;
- (ii) extracting M_I from M ;
- (iii) constructing V_{Cert} by applying V^I_{Start} to M_I ;
- (iv) validating M by applying V_{CERT} to the joint signature part $S_{Cert} (M)$; if the result matches M then the server becomes operational; sending M and $S_{Cert} (M)$ to all the group servers;

(v) if, on the other hand, M is invalid, then waiting the receipt of another joint signature and in response repeating said (ii) to (iv).

23. (Cancelled)

24. (Cancelled)

25. (Currently amended) A storage medium storing computer implemented program for

providing a proactive security in proactive operating environment; the proactive operating environment includes a group of proactive servers communicating over a network; the method comprising performing the following in respect of each proactive server (PS_I) comprising:

storing in a non erasable part at least a public, non proactive related, key V^I_{start} ;

storing in an erasable part private and public data;
providing a discardable one-time private key S^I_{start} that corresponds to said public key V^I_{start} ;

providing configuration data C;
providing at least proactive services to applications;

providing a group public proactive key V_{CERT} of a corresponding private proactive key S_{CERT} ;

invoking an initialization procedure for generating
restore related information; and

invoking a restore procedure for utilizing at least
said public, non proactive related, key V^f_{start} and said restore
related information for restoring at least said public proactive
key V_{CERT} .

providing a proactive security in proactive operating
environment; the proactive operating environment includes a
group of proactive servers communicating over a network; each
proactive server (PS_i) comprising:

a storage that includes a non erasable part that
stores at least a public, non proactive related, key V^f_{start} ,
said storage further includes an erasable part for storing
private and public data; said proactive server is further
associated with a discardable one time private key S^f_{start} that
corresponds to said public key V^f_{start} ; said proactive server is
further associated with configuration data C ,

a processor for providing at least proactive
services to applications;

the proactive server is associated with a group
public proactive key V_{CERT} common to said group of proactive
servers and a share S^f_{CERT} of a corresponding private proactive
key S_{CERT} ; the method further including:

invoking initialization procedure for generating restore related information; and invoking a restore procedure for utilizing at least said public, non proactive related, key v_{start}^x and said restore related information for restoring at least said public proactive key v_{cert} .